UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,652	07/10/2003	Daniel Fremberg	911568-665-001	4150

28104 7590 02/08/2008

JONES DAY
77 WEST WACKER
CHICAGO, IL 60601-1692

EXAMINER	
LIPMAN, JACOB	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/617,652	FREMBERG, DANIEL	
	Examiner	Art Unit	
	Jacob Lipman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 1 recites that the server responds to the authentication request with a nonce, but then recites that the authentication request a hash of the nonce before it was sent. It is unclear how the client hashes the nonce before it receives the nonce.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. A medium for carrying signals is not tangible, as it can include carrier waves for example.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-21, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe et al., USPub 2004/0187024 in view of Alkhatib et al., USPub 2004/0249974.

With regard to claims 1, 6, 10, 15, 19, and 20, Briscoe discloses an authentication protocol for increasing safety against a computer access attack for point-to-point communication ([0010]), between a client computer and a server ([0002]), to services in at least one of a network for data and telecommunication utilizing a challenge-response pattern ([0016]), including receiving from a client computer an authentication request containing a clients username to a server providing the services (secret signature), the server identifying the client computer IP address and a client password accessible by the server through the transmitted username (Fig 3) the server responding with an N byte nonce numerical value (issuing network entity [0045), the authentication request including a hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and the nonce value ([0045]) receiving the hash value from the client computer as an authenticator for accessing the services ([0046]) and the server reproducing the authenticator by utilizing the hash algorithm and the parameters clients accessible password, client computer unique IP address, server unique IP address, and the nonce value, comparing the reproduction with the transmitted authenticator, and granting an access to the server and services if the reproduced authenticator matches the transmitted ([0064]). Briscoe does not teach using this protocol to prevent a man-in-the-middle attack. Further, Briscoe teaches

using the same method for a client to verify the server ([0046]). Alkhatib discloses using a seed to thwart man-in-the-middle attacks ([0151], [0158]). The seed of Alkhatib is combined with the IP addresses in a similar manner as Briscoe. It would have been obvious for one of ordinary skill in the art to use the "cookie" of Briscoe to thwart the man-in-the-middle attack of Alkhatib since it is irreproducible by other parties, the stated motivation of Briscoe ([0046]).

With regard to claims 2 and 11, Briscoe discloses using a time parameter to create the nonce ([0046]), thus it will be different every time.

With regard to claims 3 and 12, Briscoe discloses that the seed of the nonce is random ([0044]).

With regard to claims 4, 5, 13, and 14, Briscoe discloses the nonce includes a password (Ka) and a volatile value (timestamp) ([0046]).

With regard to claims 7, 8, 16, and 17, Alkhatib discloses HMAC-Sha-1 is a known hash function ([0133]). It would have been obvious for one of ordinary skill in the art to use SHA-1 as the hash function of Briscoe since it is a widespread standard and secure.

With regard to claims 9 and 18, Briscoe in view of Alkhatib discloses the protocol of claim 1, as outlined above, but does not disclose using salt. The examiner takes official notice that using salt is well known in the art. It would have been obvious for one of ordinary skill in the art to use salt in Briscoe to protect against dictionary attacks.

With regard to claim 21, Briscoe in view of Alkhatib discloses the protocol of claim 20, as outlined above, but does not disclose identifying an attacker. The examiner takes

official notice that it is well known ion the art to log attacks and attackers. It would have been obvious for one of ordinary skill in the art to identify the attacker of Briscoe in view of Alkhatib to increase future security against the attacker.

Response to Arguments

8. Applicant's arguments filed 29 November 2007 have been fully considered but they are not persuasive.

With regard to applicant's argument that claim 1 is clear, the examiner disagrees. The claim states that server is "responding" to an authentication request with a nonce, and that the "said" authentication request included a hash of the nonce. Applicant's argument that the client "first receives a nonce" does not correspond to the claims specifically stating that the nonce is sent in response.

With regard to applicant's argument that a signal carrying medium must be tangible since it is sent between two tangible machines, the examiner points out that carrier signals are also sent between two tangible machines, but they are still intangible.

With regard to applicant's argument that the instant application has several advantages over the prior art, the examiner points out that the claims still read on the references, as outlined above. Applicant is urged to argue specific limitations written in the claims that do not read on the references.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob Lipman whose telephone number is 571-272-3837. The examiner can normally be reached on M-Fr.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER
02/06/08